

## **REMARKS**

Claims 1-24 are all the claims pending in the application. The Examiner rejects independent claims 1, 10, and 22 under §112, second paragraph as being indefinite for failing to point out and distinctly claim the subject matter of the invention. Claims 1, 2, 4, 9-11, 14, and 21-23 are rejected under 35 U.S.C. §102(b) as being anticipated by Wasilewski (US 5,420,866) in view of Applied Cryptography, Bruce Schneier; claims 3, 12, and 13 under 35 U.S.C. §103(a) as being unpatentable over Wasilewski in view of Mroczkowski ("Implementation of the block cipher Rijndael using Altera FPGA," May 2000); and claims 5-8, 15-20, and 24 as being unpaentable over Wasilewski in view of Daemen ("AES Proposal: Rijndael," March 1999).

Applicant amends claims 1-6, 10-11, 14, 22-23, and 24.

### **Oath/Declaration**

A correct Oath and Declaration is concurrently submitted showing the inventor's citizenship as South Korea along with a Petition under 37 CFR 1.47(b)  
– Unavailability of Inventor and supporting documentation.

### **112 Second Paragraph Rejections**

The Examiner rejects claims 1, 10, and 22 for indefinite terminology, specifically between "block data," "block units," "byte data," and "byte units." Applicant has amended the terminology in claim 1 to recite only "bytes" as being a data stream wherein the data stream is converted into "data blocks" for encrypting or decrypting, and wherein "data blocks" are reconverted to a data stream of "bytes" after encryption or decryption. Claims 10 and 22 do not recite "block data," "block units," "byte data," and "byte units," but recite a first format and a second format instead. Applicant believes the 112 rejections should not apply to claims 10 and 22. Amendments to dependent claims 11 and 23 similar to the amendments to claim 1 have been made to overcome the 112 rejections.

Regarding claim 1, applicant has amended “outputting the converted block data of the bytes unit” to “outputting the bytes.”

Regarding claim 1, the Examiner has indicated claim 1 omitted the essential step of encrypting or decrypting. Applicant respectfully disagrees. The control unit converts the data stream from bytes into data blocks, and passes the data blocks to the block round unit for encryption or decryption. The description of the block round unit included the limitation “so as to carry out the encryption or decryption.” Applicant believes this limitation supplies the essential step of encryption or decryption, but has amended this limitation to recite “encrypting or decrypting the received block data.”

Applicant believes all the Examiner’s rejections have been addressed with these amendments, and respectfully request reconsideration and withdrawal of the rejection.

**102(b) Rejections**  
**Wasilewski and Schneier**

“A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.” *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). See, MPEP 2131.

**Claims 1, 10, and 22**

Independent claims 1, 10, and 21 stand rejected under 35 U.S.C. §102(b) as being anticipated by Wasilewski in view of Schneier. The Examiner states that Wasilewski teaches encrypting data with the DES protocol, and Schneier teaches that the DES protocol uses a key scheduling unit carrying out a key schedule every round.

Applicant amends claims 1, 10, and 22 to recite “a variable key size so as to output a key for the encryption or decryption for each round, wherein the

variable key size is one of 128, 192, and 256 bits." Schneier teaches that DES uses a subkey having a fixed size (48 bits) that is generated for each round, and that the size of the subkey is never changed. For example, Schneier states clearly on page 272 that the 64-bit DES key is initially reduced to a 56-bit key by ignoring every eighth bit, and a different 48-bit subkey is generated for each of the 16 rounds of DES. The difference between DES and the present invention is that DES uses a fixed 56 bit key for encryption while the invention described in this application uses 128, 192, or 256 bits for stronger encryption. These amendments find support in the specification in paragraphs starting with 0035.

In view of the above amendments and remarks, applicant believes independent claims 1, 10, and 22 are now allowable, and respectfully requests reconsideration and withdrawal of the rejection.

**Dependent claims 2-9, 11-21, and 23-24**

Each of the above listed dependent claims depends from a now allowable independent claim and is therefore allowable for at least this reason. Applicant respectfully requests reconsideration and withdrawal of the rejections.

**103(a) Rejections**  
**Mroczkowski and Daemen References**

**Claims 3, 5-8, 12-13, 15-20, and 24**

Each of these claims is rejected under 103(a) as being unpatentable over Wasilewski in view of one of Mroczkowski and Daemen, each of which are directed towards encryption systems. However, neither Mroczkowski nor Daemen teaches "a variable key size so as to output a key for the encryption or decryption for each round, wherein the variable key size is one of 128, 192, and 256 bits" as required by independent claims 1, 10, and 22 from which claims 3, 5-8, 12-13, 15-20, and 24 depend.

For at least this reason as well, applicant believes claims 3, 5-8, 12-13, 15-20, and 24 are patentable as well, and respectfully requests reconsideration and withdrawal of the rejection.

**CONCLUSION**

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain at issue which the Examiner feels may be best resolved through a telephone interview, the Examiner is kindly invited to contact the undersigned at (213) 623-2221.

Respectfully submitted,

Lee, Hong, Degerman, Kang & Schmadeka

Date: July 3, 2007

By: \_\_\_\_\_

  
\_\_\_\_\_  
Craig W. Schmoyer  
Registration No. 51,007  
Attorney for Applicant

Customer No. 035884